June 3, 2019

Donald Rucker, M.D.
National Coordinator for Health Information Technology
Department of Health and Human Services
Attention: ONC 0955-AA01
330 C Street NW
Washington, DC 20201

Re: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Dear Dr. Rucker:

On behalf of the over 80,000 members of the American College of Surgeons (ACS), we appreciate the opportunity to submit comments to the Office of the National Coordinator for Health Information Technology (ONC) 21st Century Cures Act: Interoperability, Information Blocking and the ONC Health IT Certification Program Proposed Rule published in the Federal Register on March 4, 2019. The ACS is a scientific and educational association of surgeons, founded in 1913, to improve the quality of care for the surgical patient by setting high standards for surgical education and practice.

Overview

The ACS puts the welfare of our surgical patients above all else, and we support policies and regulations that promote high-quality care, reduce the regulatory burdens placed on physicians, streamline clinical workflow, and empower patients with data. As ONC engages in efforts to increase innovation and competition by giving patients and their healthcare providers secure and seamless access to electronic health information, this proposal presents very real challenges and possible unintended consequences which ONC must carefully address before the conceptual model can have a positive impact on patient care. ACS, with its 100 year history in establishing standards for the national improvement of surgical care, stands ready to collaborate with ONC to work towards patient-centered interoperability. Improving access to patient data is critical, but
what is even more important is ensuring that we are moving the right data, in the right way, and to the right person. In our letter, we highlight the following high-level comments that we believe will work to achieve the intent of 21st Century Cures Act:

- **The proposed interoperability conceptual model needs testing before national implementation.** While ACS supports the conceptual model, ONC should not begin wide-spread implementation without initial pilot testing. There are too many factors, including new third party developers, updated standards that may be new to many vendors, and resource-heavy implementations for providers, to move forward with implementation. Additionally, we ask for clarification of the process, including the expected role(s) of all stakeholders. For example, is it expected that the provider will act as agent of the patient in gaining access to patient data from third-parties?

- **Privacy and security regulations need to be updated for the modern digital landscape.** ACS encourages regulators to come together to explore a rewrite of the policies for protecting patients in a digital Protected Health Information (PHI) ecosystem, including the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security, Institutional Review Board (IRB) regulations, 42 CFR Part II, and the Common Rule. The current privacy and security regulations were created without the endless possibilities of data exchange made possible under the 21st Century Cures Act. Further, given the budget cuts to ONC and the Office for Civil Rights (OCR), as currently proposed in the Trump administration’s 2020 budget plan, we question the agencies’ resources to implement and enforce the framework proposed, complicated further by new information blocking standards amidst the unaddressed privacy and confidentiality concerns.

- **ACS encourages that the certification of technology and clinical logic be a requirement for third-party developers and their products.** As third party developers in the health space grow, ACS is concerned about the efficacy of the clinical content and algorithms in new applications. Because ONC has not provided guidance on how and if the clinical models, the algorithms, and the technical executable logic will be validated, verified, and certified, ACS is worried about the expectations that could be put on clinicians to send patient health data to an application without any form of clinical assurances. Similar to how the Food and Drug
Administration (FDA) has a certification and regulatory process in place for mobile applications, the ACS recommends that these criteria be adjusted and adopted in order to authenticate application developers.

- **ACS supports the varying levels of interoperability and adoption of standards.** We appreciate that this proposed rule recognizes the multi-faceted nature of interoperability challenges, as well as acknowledgement of the current lack of standards or consistency across platforms. Adoption of Application Programming Interface (APIs) and standards, such as Fast Healthcare Interoperability Resources (FHIR) and US Core Data for Interoperability (USCDI), aim to address many technical challenges, while the information blocking and other fee-related restrictions work to create a more level playing field.

- **ACS supports the platform to platform interoperability framework, grounded in open source digital standards.** Platform to platform interoperability partnered with required standards for data exchange will better enable bidirectional exchange, particularly when facilitated through a common patient data model in a single cloud platform, as illustrated in Figure 1 below.
- **Policies should enable the data flow of relevant and critical data, not all data.** Improving access to data is critical, but it is even more important to ensure that we are moving the right data, in the right way, and to the right person or product. Focusing on too large of a volume will result in patients being overwhelmed with unexplained and unnecessary data and with physicians struggling to sift through excess information quickly enough for point-of-care decision-making. The ACS has remaining questions about how to meaningfully filter information for care without overwhelming the system with information, and suggests limiting data exchange to meaningful and standard data elements.

- **The ONC should closely monitor provider burden and ensure these proposed changes will not result in adverse effects.** The updated regulations will shift the data landscape in healthcare, and will result in patients having unprecedented, and likely unexpected, access to health information. This health information will include additional clinical information, including lab and procedure results, notes, and more; this will likely result in an increased volume of questions to providers and care teams. As this expansion of information also grows to include payer and claims data, providers and patients alike will have questions regarding these data and what it means for care. ACS is concerned about the increased volume and expectations that access to these data will result in for providers, particularly amidst the already increased administrative burden that came with Electronic Health Record (EHR) use and adoption. It is critical that HHS’ policies evolve with these changes and demands on providers’ time.

- **Patient and provider education is critically needed.** Federal agencies have an obligation to work together to assist with education and to set standard terms and conditions to ensure that patients understand what they are agreeing to when consenting to share health information, including: how their information could be used, which organizations are required to comply with HIPAA, and which are not. These duties should not fall on the shoulders of providers. Additionally, it is important for federal agencies to educate the physician community about these new data sharing risks, as well as what role and obligations the physician has in terms of making data available, authenticating the identity of requestors of data, and otherwise authorizing access to data. It is equally important that the federal government set parameters for the appropriate use of data by third-party entities. Patients engage
with clinicians for their care and have no sense of how their PHI is transmitted and used in their care decisions by other clinicians, such as payer-employed administrators. Patients should have control over who reads and uses their PHI and who sells their PHI for secondary gains. It is imperative that patients fully understand the implications of sharing their data with third-party entities that are non-covered HIPAA entities and the potential for data to be commercialized or misused in ways that can impact coverage, access to care, and interfere with the physician-patient relationship.

Our comments below are presented in the order in which they appear in the rule.

**Deregulatory Actions for Previous Rulemaking**

**Removal of Randomized Surveillance Requirements**

ONC-Authorized Certification Bodies (ONC-ACBs) are currently required to conduct surveillance (both reactive and randomized) of certified health IT under the Program. ONC proposes to eliminate the requirement to perform randomized in-field surveillance. ONC-ACBs would still be required to perform reactive surveillance, and would be permitted to conduct randomized surveillance of their own accord. ONC claims this proposal would reduce provider burden since providers have expressed concern about the time commitment to support ONC-ACB randomized surveillance of health IT products, particularly if no non-conformities with certified health IT were found.

ACS shares ONC concerns and efforts to reduce provider burden. However, a reactive surveillance program creates provider burden. ACS prefers continued reaction and random surveillance with the burden shifted to the program developers and vendors, not to the clinicians.

**Development of Similar Independent Program Processes- Request for Information**

To reduce burden and promote innovation, ONC requests comment on whether it should establish new regulatory processes that would recognize the unique characteristics of health IT by looking first at the health IT developer (as a whole), rather than primarily at the health IT presented for certification, as is currently done under the Program. This is similar to the FDA’s current Software Precertification Pilot Program, which recognizes the unique characteristics of medical products that rely on digital
technology by looking first at the firm, rather than primarily at each product of the firm. For example, ONC could possibly establish Conditions and Maintenance of Certification requirements that would deem all of a health IT developer’s health IT as “certified” under the Program (ONC clarifies this would apply only to “functionally-based” certification criteria and not criteria that are essential to interoperability, such as the “CPOE” criteria). This approach could rely on, but not be limited to, one or more of a combination of the following: certain demonstrated health IT developer processes or health IT functionality; prior successful certification under the Program; results of real world testing; the results of the EHR Reporting Program once implemented, etc.

As recommended multiple times throughout the draft, the 21st Century Cures legislation has created a clear need for standards and certification for developers of HIT, and HIT products. The ACS recommends that the ONC develop the following types of standards for the certification of the HIT product—we believe the actual product that is deployed for use in the marketplace requires certification:

- **Privacy Certification**: this is necessary so that the app user has confidence that the app meets certain privacy standards. It is critical to clarify what happens to Electronic Health Information (EHI) that is covered under HIPAA once it is sent to a mobile app.
- **Clinical Logic Certification**: certification of the clinical logic used to ensure that the products are safe, accurate, and in alignment with clinical guidelines. We encourage ONC to leverage the expertise of professional society organizations to certify the clinical logic. We believe that third-party app developers should be held responsible for medical errors. Certification of technology and clinical logic would largely eliminate this concern for users and developers of apps.
- **Certification of Technology**: API technology certification is essential for achieving more scalable and efficient interoperability. More importantly, we support ONC’s proposal to require the industry to adopt APIs that rely on standards such as FHIR and the USCDI.

**Updates to the 2015 Certification Criteria**

ONC proposes multiple important updates to the 2015 Edition Certification Criteria to advance interoperability, some of which are discussed below. If these updates are finalized, the ACS recommends that ONC update the name of the criteria for simplicity (e.g. “2019 Edition..."
Certification Criteria” or “2015 Edition Certification Criteria 2.0”). An updated title would help physicians distinguish between products with older functionalities versus newer functionalities that allow them to more easily comply with the data access requirements set forth in this rule, as well as programs such as the Merit-Based Incentive Payment System (MIPS).

ACS encourages ONC to develop EHR certification standards to be compliant with the described open source digital standards that meet criteria for clinical interoperability. This would greatly aid in data liquidity, which would largely eliminate data blocking, and enable patient cloud environments. Further, updated standards should include the ability for EHRs to ingest external data after clinical reconciliation, allowing for a complete health record for the patient within a provider’s single system. Requiring data be sent and received in a single, standard format will better enable bidirectional exchange, particularly when facilitated through a single cloud platform, as illustrated in Figure 1 below.

Figure 1:

Timing of Implementation

For many of the policies discussed below, ONC proposes that health IT developers with existing federally certified products update their certified health IT and provide the updated certified health IT to all their customers no later than 24 months after the effective date of the final rule. Some
proposals would also require physicians to deploy updates within the same 24-month timeframe. Although there is a critical need for updated functionalities that support interoperability, we have serious concerns that if ONC holds health IT developers to an aggressive timeline, it could result in updated products that have poor functionality and cumbersome user interfaces—all due to the lack of time to properly test these functionalities. It is more important to implement changes correctly than to implement them rapidly.  

**Furthermore, as we discuss below, physicians should not be held to the same timeline as health IT developers because they will need time to research which updated products to invest in and then deploy those systems in their practice.** Rushed and poorly-informed decisions can result in the adoption of ill-suited systems that could both frustrate clinicians with cumbersome workflows, or potentially lead to patient safety issues.

**Revised and New 2015 Edition Criteria**

*The United States Core Data for Interoperability (USCDI) Standard*

ONC discusses the limitations of the previously adopted “Common Clinical Data Set” (CCDS), which encompasses a common set of data types/elements and associated vocabulary standards used currently to identify electronic health information for access, exchange, and use across several certification criteria. In order to increase the minimum baseline of data classes that must be commonly available for interoperable exchange, ONC proposes that health IT developers be required to update their certified health IT to instead support the **United States Core Data for Interoperability (USCDI v1) standard** for all certification criteria affected by this proposed change. The USCDI standard consists of data classes, which are further delineated into groupings of specific data element(s). It includes laboratory results and tests, medications, health concerns, assessment and plan of treatment, care teams, clinical notes, and other data points needed for care coordination. Existing certified EHRs would have to incorporate the USCDI standard no later than 24 months after the effective date of the final rule.

Later in this rule, ONC proposes that API technology made available by health IT developers would need to support the equivalent data classes specified in the USCDI v1. CMS also proposes in its own rule to require that data elements made available by health plans through API technology be consistent with USCDI v1 and that plans exchange, at a minimum, the USCDI v1 data set at enrollee request.
In general, ACS supports the expansion of baseline data that must be made available for interoperable exchange by certified EHRs. We are encouraged by remarks by both ONC and CMS that the USCDI is well-positioned to facilitate care coordination and to promote interoperability and appreciate ONC’s intent to update and expand this set of data classes on an annual basis using a process that is predictable, transparent, and based on public input. However, we question whether 24 months is a sufficient amount of time for health IT developers to incorporate this new standard and ensure that it is working effectively, particularly to add new data elements, such as clinical notes. As ONC continues to expand the USCDI, broad scale pilot testing is needed to evaluate the feasibility and uptake of these changes, including barriers to implementation that may arise due to the incorporation of new technologies, treatments, and care plans. We also recommend that ONC provide health IT vendors more time to conduct real-world testing of updated standards before requiring full implementation, as well as testing time for health information exchanges (HIEs) to ensure they can accept and share updated data points.

ONC highlights specific advantages of the USCDI over the CCDS, including the following:

- **Clinical Notes.** The USCDI v1 includes a new data class, titled “clinical notes.” ONC recognizes that a number of different clinical notes could be useful for stakeholders and considered multiple options for identifying the different “note types” to adopt in USCDI v1. It ultimately proposed to set a minimum standard of eight note types as a minimum bar. Specifically, ONC proposes to include the following clinical note types for both inpatient and outpatient (primary care, emergency department, etc.) settings in USCDI v1 as a minimum standard:
  - Discharge Summary note
  - History & Physical
  - Progress Note
  - Consultation Note
  - Imaging Narrative
  - Laboratory Report Narrative
  - Pathology Report Narrative
  - Procedures Note

“Clinical notes” is something many specialties have long flagged as important in the context of exchanging electronic medical data, and we appreciate ONC considering this new data class. Since existing clinical
notes range in format—e.g., some are composed of text generated from structured (pick-list and/or check the box) fields while others are in the form of unstructured (free text) data—we again urge ONC to conduct broad scale testing on the extent to which these new data classes are feasibly and accurately available in the context of interoperable exchange, and to understand from providers if they find the format and content useful to their workflow. One key issue for ONC to consider is what knowledge may be lost in the process of standardized notes, and if this loss is worth the ability to exchange standardized notes. We would also appreciate clarification on whether these data classes and types are one-size-fits-all or specific to the case type. If not the latter, then we would strongly encourage ONC to develop case type clinical notes.

- **Provenance.** The USCDI v1 also includes a new data class, titled “provenance,” which describes the metadata, or extra information about data, that can help answer questions such as when and who created the data. ONC proposes to delineate the provenance data class into three data elements:
  - The author, which represents the person(s) who is responsible for the information;
  - The author’s time stamp, which indicates the time the information was recorded; and
  - The author’s organization, which would be the organization the author is associated with at the time they interacted with the data.

ACS agrees that information on the provenance of clinical data is valuable for interoperable exchange and fundamental for improving the trustworthiness and reliability of the data being exchanged. It is especially critical in the context of APIs, as it provides an audit trail of data, preserving important details in order for the recipient to better understand the origin of the data. For example, if you do not have the metadata, it is not possible to know who wrote the notes, why they were written, when clinical notes originated to inform how recent the data is and if it is clinically relevant, etc. As data are increasingly collected from alternative sources, such as phones and wearable devices, it is critical to maintain a complete picture of the various entities and stakeholders, including patients, who contribute to the gathering of that data. It is critical that data provenance not only adhere to standards, but also be accessible, readable, and actionable by recipient stakeholders.

- **Unique Device Identifier(s) for a Patient’s Implantable Device(s).** ONC acknowledges that a recently published implementation
guide (IG) within HL7 provides further guidance on unique device identifier (UDI) requirements and identifies changes needed to the HL7 Consolidated Clinical Data Architecture (C-CDA) to better facilitate the exchange of the individual UDI components in the health care system when devices are implanted in a patient. The UDI components include the Device Identifier (DI) and the following individual production identifiers: the lot or batch number, serial number, manufacturing date, expiration date, and distinct identification code. Because UDI’s were developed in order to track patient implantables for critical patient safety issues, ONC should require the UDI IG in order to meet the USCDI standards. This is precisely why UDIs were created--if a patient has a device and it turns out that device has a problem, it is critical that we can track and identify those patients.

Electronic Prescribing Criteria

ONC proposes to update the electronic prescribing (e-prescribing) SCRIPT standard, which would result in a new e-prescribing standard eventually becoming the baseline for certification. ONC states that this proposal would harmonize with relevant CMS programs that have finalized the updated SCRIPT standard, including the Part D e-prescribing requirements and the option for clinicians, hospitals, and Critical Access Hospitals (CAHs) to report on the Query of Prescription Drug Monitoring Program (PDMP) quality measure for the Promoting Interoperability Programs.

ACS supports the intended goals of updating the new e-prescribing SCRIPT standard, in addition to any efforts to improve patient safety and prescription accuracy, create workflow efficiencies, reduce testing requirements, and increase configurability of systems. We also support the efficient and accurate exchange of medication history transactions between providers and pharmacies, and between pharmacies and state PDMPs. If the new e-prescribing SCRIPT standard addresses these important goals, we support the use of the new standard.

However, we continue to have concerns with the Query of PDMP, which will measure the use of data from CEHRT to conduct a query of a PDMP for Schedule II opioid prescriptions. The ACS supports the intent of this measure as we believe the use of PDMPs must be bolstered to fight against the opioid epidemic, but we do not support the measure as written and support that the measure remains an optional bonus measure for the 2020 performance year, as proposed by CMS in the
IPPS proposed rule.

PDMPs, which are statewide databases that collect information on the distribution of controlled substance prescriptions, can be used to track opioid prescriptions in some manner in all states except for Missouri. While the ACS has promoted the use of PDMPs to inform clinical decision-making and facilitate intervention at the point of care, we remain concerned that PDMP data are not standardized and are poorly integrated into existing workflows. Further, each state with an established PDMP has its own set of laws governing what type of drug use data are available, what type of prescriber can access the PDMP, and how the data are shared. Currently, PDMPs largely operate as outdated repositories that do not provide physicians with the real-time, actionable information needed to determine a patients’ pattern of prescription drug purchase or prior therapies. In addition, PDMPs do not effectively share data across states, enabling patients who live near state borders to duplicate prescription purchases in each state without the prescribing physician’s knowledge. As a result of these inefficiencies, in many states, checking PDMPs is cumbersome, time-consuming, and may yield incomplete information.

To combat this widespread issue, CMS and ONC should work towards making one national standard for PDMPs and reward clinicians who use the national standard. As CMS and ONC work toward this goal and to ensure that PDMPs are used more consistently and universally across the nation, the agencies should also work with vendors to amend the EHR certification process and other secure, mobile digital health information systems so that it includes rules about PDMP queries and data exchange. Until these issues are addressed, we remain concerned about the use of the Query of PDMP measure in CMS’ Promoting Interoperability programs.

Electronic Health Information (EHI) Export

ONC also proposes to require, through updated 2015 Edition certification criteria, that health IT developers provide the capability to electronically export all EHI they produce and electronically manage in a computable format. Specifically, this criterion would:

- Enable the export of EHI for a single patient upon a valid request from that patient or a user on the patient’s behalf;
- Support the export of EHI when a health care provider chooses to transition or migrate information to another health IT system; and
• Require that the export include the data format, made publicly available, to facilitate the receiving health IT system’s interpretation and use of the EHI to the extent reasonably practicable using the developer’s existing technology.

ONC clarifies that EHI export encompasses all the EHI that the health IT system produces and electronically manages for a patient or group of patients. This applies to the system’s entire database, including but not limited to clinical, administrative, and claims/billing data. “EHI” also includes the oldest EHI available on that patient to the most recent, no matter the specific electronic format (e.g., PDFs are included). ONC proposes that health IT developers must implement this capability within 24 months of the final rule's effective date.

**General Comments**

The ACS very much appreciates that this proposal aims to provide patients and health IT users, including providers, a means to efficiently export the entire electronic health record for a single patient or all patients in a computable, electronic format. Switching EHR systems is an especially time consuming and resource-intensive activity for physicians that often results in lost or non-discrete data. We also appreciate that this criterion would provide additional assurances that a health IT developer supports, and does not inhibit, the access, exchange, and use of EHI. Importantly, this proposal also supports longitudinal data record development, which will help to foster better care coordination and more efficient care over time.

Over a longer-term, we support requiring developers to build systems that can readily export data as a standard capability of certified health IT. However, for the more immediate future, we are concerned that ONC is setting too ambitious of a goal with this proposal and failing to recognize important attributes that must first be in place to ensure successful implementation. **For example, ONC is not proposing that the export must be executed according to any particular standard. It is only requiring that the export must be accompanied by the data format, including its structure and syntax, to facilitate interpretation of the EHI.** It is critical that there are standards to export data in order to ensure the data are pulled consistently from every system, and that it could then be imported and integrated into other systems as needed. We are very concerned that the absence of standards will pose a major obstacle to transferring EHI between EHR systems. This proposal also focuses exclusively on the ability of support complete health records and more
informed decision-making. This is a particular problem for patient-generated data, as it has the capacity to be extensive and in a variety of formats in the absence of a standard. Furthermore, we seek clarity on how ONC expects health IT vendors to develop the capability to feasibly export all EHI, especially considering the limited scope of FHIR resources. For example, large, national vendors, such as Epic, have about 60,000 data fields in their systems. However, only about 3,000 of those are supported by FHIR-standards and approximately 10,000 are currently being converted for use as FHIR resources. The remainder of the fields are not in a computable format, including scanned images, audit trails, and other data elements that would not be beneficial information for the course of treatment. Furthermore, it is unrealistic to expect a successful rollout of this ambitious proposal within a short 24-month timeframe.

The ACS strongly recommends that ONC adopt uniform standards that certified health IT developers would have to adhere to ensure that data can not only be exported, but also imported by the receiving entity. We also request that ONC clarify how it expects vendors to export large portions of their data that are not yet supported by FHIR-standards and easily transferable: will this be done by creating a series of translators to convert data into computable, discrete format (e.g., HL7 v1, v2, FHIR, etc.)? Furthermore, we request that ONC clarify the intersection between its data export proposal and its API proposals, including the extent to which APIs would facilitate data export. Finally, we request that ONC reconsider the 24-month implementation timeframe in light of all these concerns. As noted throughout this comment letter, it is more important to carry this out effectively than quickly. Rushed deployment runs the risk of exporting data in a format that is useless to physicians and patients, negating the entire value of this proposal. Extending the timeline and limiting the initial data set subject to this requirement to USCDI standards will result in a much more manageable mandate for health IT developers and help to minimize potential unintended consequences that could interfere with the goals of this proposal. ACS recommends that vendors and developers be given 18 months for development, allowing for a 2021 implementation, and providers and health systems are given 24 months beyond that to upgrade and incorporate these updated standards. After this has been piloted with the USCDI format, we recommend working with an advisory group of providers and vendors to determine the additional data elements that would be useful in clinical care and care management to include beyond the USCDI framework.
Scope of EHI

For both use cases supported by this criterion, ONC clarifies that the clinical data that would have to be made available for export would encompass imaging information – both images and narrative text about the image. However, ONC understands that EHRs may not be the standard storage location for images and solicits comment on the feasibility, practicality, and necessity of exporting images and/or imaging information. While we agree that standardized electronic imaging data has not yet been widely integrated into EHRs, ACS urges ONC to work with relevant stakeholders to accelerate the incorporation of Digital Imaging and Communications in Medicine (DICOM)-based images into certified health IT, into the USCDI, and into the nation’s broader interoperability framework. DICOM is a long-established standard that, among other things, supports the interoperable exchange of medical images. Currently, the USCDI v1 only includes the imaging narrative, but not the image itself. While the imaging report provides important information, surgeons need reliable access to the actual image to provide the highest quality care. Greater accessibility to imaging data will help to ensure that surgeons are better stewards of imaging resource use.

Understanding that developers are not able to export every existing data element, nor that all possible data elements are necessary for transfer, ONC also seeks comment on whether, in the future, it should require that health IT developers attest or publish as part of the export format documentation the types of EHI they cannot support for export. While the Certification Program should continue to put pressure on health IT developers to make as much data as is feasible available for electronic export, we support this proposal as an interim solution to enhance transparency and assist physicians when deciding on which systems to invest. Further, ACS recommends creating an advisory group that includes both providers and vendors to recommend the fields that should be included in the EHI standard, in order to ensure that the standard allows a pathway for data to be importable and integrated, and that they are necessary and important for improving the standard and quality of care.

Privacy and Security Transparency Attestations

This rule proposes to update the 2015 Edition certified EHR technology (CEHRT) by proposing criteria for removal, as well as revisions to the current criteria and new criteria for the certification of health IT. The comments below focus on the two proposed new privacy and security transparency attestation certification criteria.
The ONC proposes to require that a Health IT Module developer identifies whether their certified health IT supports encrypting authentication credentials and/or multi-factor authentication. In order to be issued a certification, ONC proposes to require that a Health IT Module developer attest to whether the module encrypts authentication credentials and whether it supports multi-factor authentication. ONC explains that it believes certification to these proposed criteria would provide increased transparency and potentially motivate health IT developers to encrypt authentication credentials and support multi-factor authentication, which could prevent exposure to unauthorized persons/entities.

ACS believes that privacy and security should extend to a patient’s digital PHI no matter where it resides, and therefore this proposal does not go far enough to establish those assurances. For example, under the ONC proposal, how does Epic or Cerner assure that an API developer can authenticate that someone using their API or connected third-party application has the right credentials to access PHI? How is it authenticated that the clinicians who works for that specific hospital that has Epic, is assigned to a specific patient? This proposal highlights a central theme throughout this letter, which is encouraging regulators to come together to explore a complete rewrite of the policies for protecting patients in a digital PHI ecosystem, including HIPAA Privacy and Security, 42 CFR Part II, IRB regulations, and the Common Rule. The current privacy and security regulations were created without the endless possibilities of data exchange made possible under the 21st Century Cures Act. One option is for HHS to create a digital health privacy and security commission to oversee this work.

ONC also proposes updated criteria that would support a more granular approach to privacy tagging data consent management for health information exchange. These criteria aim to allow providers to share portions of an electronic medical record while not sharing others, such as information that is given heightened protection under the law. ACS supports the proposal to allow for a more granular approach to privacy tagging data consent management, but we urge ONC to clarify that this should be tailored to patient preferences—this technology should allow for a system to share certain information that the patient has indicated he/she wants to share. However, ACS is concerned that given 42 CFR Part II regulations and the multiple consents required from patients to share information that crucial clinical information could be missing from the medical record in the absence of
standardized tracking of patient consent. ACS further recommends updating 42 CFR Part II to align with updated standards for data sharing and interoperability, as well as implementing a standard system for tracking patient consent, such as Consent2Share, which is an open source software application that allows patients to determine, through an online consent process, which health information they would like to share and not share with their providers.¹

**Health IT for the Care Continuum**

**Health IT and Opioid Use Disorder Prevention and Treatment – Request for Information**

ONC seeks comment on whether current certification requirements and proposals in this rule may support use cases related to Opioid Use Disorder (OUD) prevention and treatment, and if there are additional areas that ONC should consider for effective implementation of health IT-enabled OUD prevention and treatment.

*Revised or New 2015 Edition Certification Criteria in this Proposed Rule*

The ACS seeks to assure that surgical patients continue to have adequate pain control and receive the proper postoperative care needed to restore their overall health and avoid prescription opioid-related complications. We believe that surgeons have a responsibility to minimize their patients’ postoperative pain while addressing the societal imperative to avoid overprescribing, and in 2017 developed the following five principles to guide our efforts in preventing opioid abuse and addiction in surgical patients:

ONC described several revised or new 2015 Certification Criteria in the proposed rule that can also support treatment and prevention of OUD:

- **The USDCI standard.** This standard would establish a minimum set of data classes that are required to be interoperable nationwide. It includes data elements such as “medications” and two new data classes titled “clinical notes” and “provenance,” which are expected to enhance the comprehensiveness and reliability of the data being exchanged and could help empower physicians in the prevention and detection of opioid misuse, abuse, and diversion. This additional information will aid providers in making the best clinical care choices for their patients.

- **Electronic Prescribing and PDMPs.** ONC’s proposal to adopt new electronic prescribing certification criterion can help address current challenges related to e-prescribing by supporting improved patient safety and prescription accuracy, creating workflow efficiencies, reducing testing requirements, and increasing configurability of systems. It supports the efficient and accurate exchange of medication history transactions between providers and
pharmacies, and between pharmacies and state PDMPs. This new proposed criterion also includes the addition of Risk Evaluation and Mitigation Strategy (REMS) messages.

Integration of PDMPs into the clinical workflow have the potential to greatly improve feasibility of checking patterns of patient opioid prescription purchases and thereby increase utilization of the PDMP by providers. If the proposed new e-prescribing criterion will address these challenges, we support the use of these and other opportunities to build upon the existing PDMP foundation and leverage health information technologies to support the functionality of PDMP data within EHRs, initiate or expand interstate data sharing, facilitate secure prescriber-pharmacy communication, and establish benchmarks to assess PDMP use.

As discussed above, ACS has promoted the use of PDMPs to inform clinical decision-making and facilitate intervention at the point of care, but we remain concerned that PDMP data are not standardized and are poorly integrated into existing workflows. Further, each state with an established PDMP has its own set of laws governing what type of drug use data are available, what type of prescriber can access the PDMP, and how the data are shared. Currently, PDMPs largely operate as outdated repositories that do not provide physicians with the real-time, actionable information needed to determine a patients’ pattern of prescription drug purchase or prior therapies (such as methadone or buprenorphine prescriptions) used to treat opioid use disorders. In addition, PDMPs do not effectively share data across states, enabling patients who live near state borders to duplicate opioid prescription purchases in each state without the prescribing physician’s knowledge. As a result of these inefficiencies, checking PDMPs is cumbersome, time-consuming, and may yield incomplete information.

The country’s opioid crisis highlights the need for digital solutions that break down data silos and provides prescribers with comprehensive, patient-specific information. Prescription history databases, whether established at the state or national level, must interact and share information to be effective and important clinical tools that will allow surgeons to better identify patients at high risk for opioid prescription abuse and tailor their prescribing behavior accordingly. An ongoing push toward standardized databases with the ability to share information across state borders is essential to ensuring physicians receive accurate information, and the ACS strongly believes that there must be
interoperability in the data contained in PDMPs with EHRs to streamline accessibility and promote patient safety.

- In this section, ONC address health IT for the pediatric setting, as well as health IT in the context of opioid use disorder (OUD) prevention/treatment.
- Section 4001(b) of the Cures Act includes two provisions related to supporting health IT across the care continuum. The first instructs the National Coordinator to encourage, keep or recognize through existing authorities, the voluntary certification of health IT for use in medical specialties and sites of service where more technological advancement or integration is needed. The second outlines a provision related to the voluntary certification of health IT for use by pediatric health providers to support the health care of children.
  - In regards to the first, ONC simply notes it has explored how it might work with the health IT industry and with specialty organizations to collaboratively develop and promote health IT that supports medical specialties and sites of service. ONC claims it has taken steps to make the Program modular, more open and accessible to different types of health IT, and able to advance functionality that is generally applicable to a variety of care and practice settings. ACS supports ONC’s efforts to promote data liquidity from EHRs to platforms whereby surgical algorithms for Clinical Decision Support (CDS) may leverage the information to create knowledge artifacts which inform patients and the entire care team. The next challenge will be how best to represent the outputs from these non-EHR platforms back to the surgeon and patient in their EHR workflows. Open APIs on these platforms based on the FHIR standards would provide a future body of work to explore. In this way, specialty medicine could continuously own and update the clinical logic in the algorithms and still provide outputs back to each instance of an EHR.
- In regards to OUD prevention and treatment, ONC seeks comment on whether emerging standards and innovations could inform future health IT policymaking:
  - **Clinical Decision Support Hooks**: ONC is currently collaborating with the Centers for Disease Control and Prevention (CDC) on a project to translate the CDC Guideline for Prescribing Opioids for Chronic Pain into
standardized, shareable, computable decision support artifacts using CDS Hooks.

- Care Plan FHIR Resource: an effort to standardize care plans using FHIR and C-CDA.

ACS supports the efforts to overcome the opioid crisis while recognizing the pain surgical patients must endure. The solutions to date have been around limiting prescriptions and seeking alternatives. In addition to prescription management, the role of technology need to be considered to enable patient engagement, education, and communication tools surrounding pain and its management. The importance of asynchronous communication using smartphone technology or the internet becomes more apparent when we realize how much care exists outside the hospital. Using third party apps to track patient-reported outcomes and pain experiences along with patient’s wound care photos and other inputs such as pulse and temperature would help patients realize and manage their pain, without feeling abandoned by a sole strategy of prescription control.

**Conditions and Maintenance of Certification**

ONC proposes multiple initial and ongoing requirements that must be met by health IT developers and their certified health IT modules, some of which are discussed below. Noncompliance with these requirements would be subject to ONC direct review, corrective action, and enforcement procedures. Overall, the ACS supports the concept of using Conditions and Maintenance of Certification requirements to set clear baseline technical and behavioral requirements, as well as ongoing assurances that these conditions are continually being met by both health IT developers and their certified Health IT Module(s) under the Program.

**Provisions**

**Information Blocking**

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, not take any action that constitutes information blocking. ONC proposes to establish this information blocking Condition of Certification, which would prohibit any health IT developer under the Program from taking any action that constitutes information blocking. Noncompliance would be subject to ONC direct review, corrective action, and enforcement procedures under the ONC Health IT Certification Program which provides additional
assurances that they will not take any action that may inhibit the appropriate exchange, access, and use of EHI. ACS supports this proposal.

Communications

Under this proposed set of Condition and Maintenance of Certifications requirements, health IT developers could not prohibit or restrict communication among users of its product(s) regarding:

- The usability, interoperability and security of the health IT;
- Users experience with the health IT;
- Business practices of health IT developers that impact the exchange of EHI.

Examples of protected communications include, but are not limited to: a post made to an online forum; the sharing of screenshots, subject to certain proposed restrictions on their general publication; an unattributed written review by a health IT user; a quote given by a health care executive to a journalist; a presentation given at a trade show; and statements and conclusions made in a peer-reviewed journal.

We thank ONC for recognizing practices that currently limit health IT users from openly discussing or sharing their health IT usage experiences. Greater transparency and open dialogue about these issues will help clinicians make more informed decisions when investing in health IT systems. It also will put pressure on developers to improve their products, services, and business practices. To strengthen this proposal, we recommend that ONC also encourage open communications about health-IT related patient safety issues, which can result from ineffective system functionalities and exchange of data. Additionally, we seek clarity on how the ONC plans to enforce this, particularly the requirement that this information is shared only among users of the system. Several of the provided examples (trade show presentation, peer-reviewed journal article) would be challenging to restrict only to users of a specific vendor’s system.

Application Programming Interfaces (APIs)

General Requirements

As required by the 21st Century Cures Act, ONC proposes to require as a Condition of Certification that health IT developers publish APIs that allow health information from such technology to be accessed, exchanged,
and used without special effort. APIs are software protocols published by one software developer that allow another developer to create applications that interact with the software without needing to know the internal workings of it. ONC specifically proposes that health IT developers would have to support API-enabled services based on FHIR standards. Through the APIs, health IT developers also would have to provide access to all data elements in the USCDI v1 that are part of a patient's EHR to the extent permissible under applicable privacy laws. ONC clarifies here that APIs developed under the FHIR standard align with the USCDI to meet these proposed certification rules. Other requirements include:

- APIs must adhere to standards that would enable and support persistent user authentication and app authorization processes;
- API Technology Suppliers must support API-enabled services for data on a single patient and multiple patients;
- API Technology Suppliers must publish the terms and conditions applicable to their API technology, including fees, and any other documentation necessary to interact with their APIs.

ONC proposes that API Technology Suppliers must develop, test, certify and make APIs available to their customers within 24 months of the final rule’s effective date. Physicians also would be required to deploy new APIs in their clinics within the same 24-month timeframe.

The ACS is a strong proponent of API technology and agrees with ONC that API technology is essential for achieving more scalable and efficient interoperability. More importantly, we support ONC’s proposal to require the industry to adopt APIs that rely on standards such as FHIR and the USCDI. Because of the focus on these standards, we recommend that the USCDI is used as a standard for EHI extracts as well, simplifying the standards in place for both vendors and users. Regarding FHIR, although current 2015 Edition criteria include API capabilities that vendors must comply with, there are currently no requirements in regard to standards, meaning the API may be the vendor’s own proprietary API. While this allows for flexibility and potentially innovation, it also presents challenges related to functional variability, which FHIR-based standards should help to address. For the USCDI standard, its specifically defined data classes and elements will further ensure consistency, efficiency, and efficacy of data exchange. We also believe that limiting the API requirements to the USCDI is a more reasonable, objective, and achievable approach compared to some of the other proposals in this rule, such as the current EHI proposal, which target a much larger universe of data. Together, these mandated standards, paired with transparency requirements, will help to
ensure foundational compatibility by providing API technology suppliers with a clear set of rules and standard data sets to adhere to when fulfilling the API requirements. They also will help to ensure uniformity for API users (e.g., patients and physicians) when attempting to integrate applications. Overall, the more widespread use of APIs that conform to these standards will help to minimize the current hodge-podge of non-scalable technology and help to remove some of the obstacles that currently stand in the way of interoperability.

ACS also strongly supports ONC’s proposal that any and all permitted fees charged by an API Technology Supplier for the use of its API technology must be published and described in detailed, plain language as part of its publicly available terms and conditions. We urge ONC to regularly enforce its requirement that the description of the fees must include all material information, including the persons or classes of persons to whom the fee applies; the circumstances in which the fee applies; and the amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee. We ask that the ONC publish the various vendor costs publicly in order to develop and enforce industry-standard reasonable pricing models. Furthermore, we appreciate that with respect to these transparency conditions, ONC proposes to establish a compliance date of six months from the final rule’s effective date. We believe this strikes a fair balance since it would give developers approximately eight months from the final rule’s publication date to revise their existing API documentation to come into compliance with the final rule.

Timing for Implementation

Despite our support for the API proposal, we have serious concerns about the overall implementation timeline. ONC calls for finishing the work on standards setting and having full health information exchange in just two years. This is an unrealistic timeline for such an incredibly complex and ambitious task. In fact, in a recent article, the CEO of HL7 International, the standards organization responsible for accelerating FHIR, seemed to be caught off guard by ONC’s proposal to require FHIR as the standard for all APIs. He warned that “[the] organization is not big enough and the mandate is out of proportion relative to the resources at [our] command,” and went on to state, “We can’t bear the intense commitment this entails
or the financial burden it brings. It’s just not possible to do it on our own.”

Just as the ACS urged ONC to slow down implementation of the Meaningful Use Program, we again encourage ONC to allow for a complete and accurate, rather than a fast, transition to this standard, particularly given the numerous potential—and serious—consequences: risks to patient privacy, patient access to care, and the erosion of the physician-patient relationship. Rushed implementation will also result in inflated costs as vendors struggle to quickly comply with all of these new mandates. Based on the concerns expressed by HL7, we also strongly encourage ONC to work with standards organizations to assess the resources needed to implement these proposals and provide the appropriate financial support. As we explain below, these costs are expected to inordinately impact providers.

Even more concerning is ONC’s proposal to require API Data Providers (e.g. physicians) to deploy this new API technology within the same 24-month timeframe that API Technology Suppliers would be required to develop, test, and certify their APIs. While we support ONC’s overall effort to stimulate interoperability and greater access to health information, it is completely inappropriate to expect providers to deploy this technology within the same timeframe as suppliers of this technology are expected to make the technology available. Based on experience with previous implementation of new EHR certification requirements, physicians and hospitals need at least 12 months to get in the install queue before their EHRs are updated. Health IT vendors will need at least 18-24 months for development. As such, the proposed 24-month timeline would leave health IT vendors with less than 12 months before their products must be made available to physicians. We request that ONC more carefully consider these realities and delay implementation for physicians to at least 24 months following the finalized API Technology Suppliers’ deployment timeline.

Key Terms and Recovery of Fees

ONC defines the following three terms in the context of APIs:

- **API Technology Supplier**: Health IT developers that create API technology presented to ONC for certification;

- **API Data Provider**: Healthcare organizations that deploy API technology created by the supplier and provides access via the API technology to data it produces and electronically manages (presumably health systems and hospitals, but also potentially physicians); and

- **API User**: Person or entity that use or create software applications that interact with the API technology (e.g., patients, physicians, and software “app” developers).

ONC also discusses what fees may and may not be charged related to data access via an API. Since physicians, in certain situations, may be an API User, we appreciate that ONC proposes fee limitations on API Technology Supplier costs for developing APIs and supporting apps. For example, API technology suppliers must treat all API Users the same. They cannot limit access or charge differently for competitors, which should help to ensure they do not abuse market power by monetizing access to data or limiting the entry of competing products. ONC also would only permit an API Technology Supplier to charge fees to API Users for “value-added services” supplied in connection with software that can interact with the API technology. Fees would not be permitted if they interfere with an API User’s ability to efficiently and effectively develop and deploy production-ready software. In other words, an API User could not be required to incur a fee in order to develop and deploy a production-ready software application that interacts with the API technology acquired by the API Data Provider. Rather, a fee will only be permitted if it relates to a service that a software developer or provider can elect to purchase, but is not required to purchase in order to develop and deploy production-ready apps. For example, API Technology Suppliers may establish additional mechanisms to assure health care providers that the apps they use within their health IT will operate appropriately, will fully integrate into workflow, and will not degrade overall system performance. Activities related to the vetting of app software would fall under the “value-added services” permitted fee.

At the same time, if we consider the role of the physician as the API Data Provider, we are concerned about the extent to which a physician would be impacted by costs and the lack of protections in terms of cost recovery. Our interpretation of these proposals is that the API Data Provider cannot charge the patient for access to the API technology, per the data blocking restrictions discussed later in this rule. However, the API Technology Supplier is allowed to recover documented and non-discriminatory costs for development and upkeep of the technology from the API Data Provider. The API Technology Supplier also can license the use of API
technology they create to recoup costs and potentially make a profit. Furthermore, as noted earlier, an API Technology Supplier is permitted to charge fees to an API User for “value-added services” supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software.

In general, the language in this section is confusing and necessitates further clarity. ACS is concerned that these proposals will leave physicians—who are mandated to use certified EHRs that include API technology and provide patients with access to data via those APIs—responsible for a variety of unwarranted costs and with little recourse to recover those costs. We request that ONC continue this discussion in an interim final rule where the public would have another opportunity to comment on clarified language before it is finalized. ONC notes in this section that “Any fee that arises in connection with an API User’s use of API technology would need to exist solely between the API Data Provider and the API User.” This seems to suggest that there might be situations when an API Data Provider can, in fact, pass on some of these costs to API Users, such as patients or third-party app developers. We would appreciate clarification on this issue. If the government is mandating the use of CERHT that includes API technology, then ONC should also provide a mechanism for HHS/ONC to cover these additional costs which will be required as part of CEHRT function. We are concerned that if fees become cost-prohibitive, providers who cannot afford the associated fees to connect with API technology will have trouble sharing patient data, which could then fall under the data blocking provisions. We would appreciate if ONC could more clearly define the scope and parameters of the various fees discussed in this section.

In this section, ONC also discusses how API Technology Suppliers would be permitted to charge API Data Providers based on the post-deployment usage activities of API Users. ONC clarifies that “usage-based” fees would not be allowed to include any costs necessary to prepare and “get the API technology up, running, and ready for use.” Usage-based fees could only be used to recover costs incurred by an API Technology Supplier due to the actual use of the API technology once it has been deployed (e.g., costs to support a higher volume of traffic, data, or number of apps via the API technology). ONC also clarifies that it expects that API usage support fees would only come into play when the API Technology Supplier acts on behalf of the API Data Provider to deploy its API technology. Conversely, in scenarios where the API Data Provider, such as a large hospital system, assumes full responsibility for the
technical infrastructure necessary to deploy and host the API technology it has acquired, the volume and scale of its usage would be the API Data Provider’s sole responsibility.

The ACS believes it is unreasonable to presume that API User-driven data overages should be the responsibility of the API Data Provider. As ONC acknowledges in the rule, this pricing model is open to abuse, with API Data Providers at risk of paying unreasonably high fees if the volume of API use is high.

ONC goes on to clarify that “the API Technology Supplier would need to be careful to ensure that the total fees paid by an API Data Provider were reasonably related to the API Technology Supplier’s costs of supporting the API technology. Where the fees paid over a reasonable measuring period were not reasonably related to the API Technology Supplier’s costs, they would not be permitted.” While we appreciate this disclaimer, the terminology in this statement is vague and open to wide interpretation. We request that ONC provide more definitive guidance, including a range of prices based on examples from the current marketplace, to ensure providers are not charged unreasonable fees by API Technology Suppliers and can reasonably charge API Users for the cost of accessing their API technology. Providers already must invest significant resources to adopt and maintain certified EHR technology. They should be recognized for this investment and for making API technologies available to patients. They should not be held responsible for costs that they have little or no control over, such as costs related to the frequency with which their patients rely on the provider’s API technology.

Application Verification Process

ONC also proposes to permit API Technology Suppliers to institute a process to verify the authenticity of application developers. This verification process would need to focus specifically on the application developer—not its software application(s). API Technology Suppliers would have the discretion to establish their verification process so long as the process is objective and the same for all application developers and it can reasonably be completed within the five business days—otherwise such a process could risk implicating/violating other elements of this proposed API Condition of Certification as well as information blocking behaviors.

ACS supports processes that would allow API Technology Suppliers to verify the authenticity of application developers; however, we recommend
that this be a requirement of certification rather than an option. Additionally, the ACS recommends that the ONC develop a standard to use for this certification. As the FDA has a certification and regulatory process in place for mobile applications, the ACS recommends that these criteria be adjusted and adopted in order to authenticate application developers. Additionally, just as critical is the 1) certification of the clinical logic used to ensure that the products are safe, accurate, and in alignment with clinical guidelines, and 2) privacy certification to ensure that apps meet privacy standards. We encourage ONC to leverage the expertise of professional society organizations to certify the clinical logic. In the current marketplace, it is our understanding that health IT developers employ hold-harmless clauses that protect them from liability if hospitals are later sued for medical errors that resulted from defects in the software. We believe that third-party developers should be held responsible for medical errors—certification of technology and clinical logic would largely eliminate this concern for users and developers of apps.

In addition, ACS suggests the ONC require an EHR vendor’s API to check for the below three “yes/no” adoption & implementation attestations as a part of the certification requirements:

- **Industry-recognized development guidance** (e.g., Xcertia’s Privacy Guidelines);
- **transparency statements and best practices** (e.g., Mobile Health App Developers: FTC Best Practices and CARIN Alliance Code of Conduct); and
- **a model notice to patients** (e.g., ONC’s Model Privacy Notice). The certified app could then be acknowledged or listed by the health IT developer (e.g., in an “app store,” “verified app” list). EHR vendors could also publicize app developers’ attestations.

Without the certification of the technology and clinical logic, the responsibility of verifying the authenticity of application developers could fall on the shoulders of API Data Providers or Users (i.e., patients and providers) who do not have the resources, time, or expertise to conduct such assessments. We appreciate ONC’s reminder that even in the case where an API Technology Supplier chooses not to vet app developers, the apps would not have carte blanche access to a health care provider’s data. Such apps would still be registered and thus identifiable and able to have their access deactivated by an API Technology Supplier or health care provider if they behave in anomalous or malicious ways. Furthermore, we support the fact that a patient seeking access to their data using the app
will need to authenticate themselves (using previously issued credentials by a health care provider or trusted source) and authorize: 1) the app to connect to the FHIR server; and 2) specify the scope of the data the app may access.

The ACS objects to policies that place a disproportionate burden on physicians in terms of resources and time, and that lack clinical and technical logic certifications. Additionally, the cost of adopting and maintaining CEHRT will inevitably rise as a result of the new requirements set forth in this rule. Since patients cannot be charged for these additional costs, providers, who are required to buy and upkeep all of this technology, will have to foot the entire bill. ACS urges ONC to more thoroughly evaluate the cost and overall impact of compliance with this and other policies proposed in this rule on the physician community. Physicians will not only be required to invest in and take the time to set up new systems, but they will also need to learn how to effectively interact with entities they have not necessarily interacted with in the past, such as app developers.

Real World Testing

This Condition of Certification would require health IT developers to annually submit real world testing plans and retrospective test results that include interoperability criteria. ONC proposes that health IT developers must test their products in the type of setting in which such technology would be marketed prior to the effective date of the final rule and provide real world tested health IT to all their customers within 24 months of the final rule’s effective date.

The ACS supports this proposal, but requests that ONC further specify that health IT developers test their products within the specific specialty to which the technology would be marketed. The lack of relevant specialty functionalities and in certified health IT products is an ongoing problem that continues to interfere with the ability of surgeons to most effectively use health IT as part of their workflow for improved patient care.

EHR Reporting Criteria for Submission

Under the Cures Act, developers are required to submit reporting criteria on certified health IT in accordance with the EHR Reporting Program. ONC has not established the EHR Reporting Program yet, and will go through the rulemaking process to establish criteria for the program. As ONC begins to think about this program, ACS encourages ONC to
incorporate criteria that informs the public about whether the product is compliant with open source digital standards, and allows for data exchange based on these standards.

**Information Blocking**

The 21st Century Cures Act defines information blocking broadly as any practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI when the entity knows it is likely to do so. It also directs the Secretary to identify actions that would not be considered information blocking and provides OIG with both investigatory and enforcement authority over information blocking. The OIG may issue civil money penalties ($1,000,000 per incident) for information blocking conducted by health IT developers of certified health IT, health information networks, and health information exchanges. The OIG may also investigate health care providers for information blocking for which health care providers could be subject to disincentives.

In this section of the rule, ONC (1) defines key terms, including EHI; (2) provides an illustrative list of activities that would be likely to interfere with access, exchange, or use of EHI; (3) codifies compliance with the information blocking provisions as a Condition of Certification; (4) introduces seven exceptions to the general prohibition on information blocking; and (5) issues a Request for Information on disincentives for health care providers.

The seven exceptions to information blocking proposed by ONC are: preventing harm; promoting the privacy of EHI; recovering costs reasonably incurred; responding to requests that are infeasible; licensing of interoperability on reasonable and non-discriminatory terms; and maintaining and improving health IT performance.

**General Comments**

Overall, the ACS appreciates ONC’s recognition that information blocking is a serious and ongoing problem and that the practice presents itself in various forms—some less obvious than others. We also appreciate ONC’s acknowledgment that health IT developers, as well as certain providers (e.g. hospitals), are in a unique position to control access to and use of EHI. Despite rights afforded under HIPAA, patients still struggle to access their health information, to transfer their records from one provider to another, and to access all of their health information in one place. Physicians also continue to face significant challenges related to
data access, including EHR vendors “locking-up” data in non-transferable formats or charging excessive fees to establish interfaces that allow physicians to use their own data in an intelligible manner, or to share their data with another EHR system or clinical data registry. Hospitals and health systems also often interfere with the sharing of data through contractual arrangements or by inappropriately claiming the need to comply with the HIPAA Rules. In light of these ongoing challenges, we thank ONC for tackling both technical obstacles, as well as systematic obstacles to interoperability such as information blocking.

However, the ACS is concerned that ONC’s information blocking definitions and proposals are vague, confusing, and subject to wide interpretation. While ONC provides an illustrative, but limited, list of activities that would likely constitute information blocking, it also clarifies that it is not possible to anticipate or catalog the many potential types of practices that may raise information blocking concerns. The ACS appreciates this challenge, but still strongly urges ONC to share with the public a more comprehensive inventory of examples of specific actions or activities that would constitute information blocking, as well as examples that have been reported over the years that required action. A more robust inventory of examples would serve as a useful benchmark for the industry to reference. Examples should be housed in a repository that is easily accessible to the public, organized and searchable by topic, and updated regularly to reflect newly identified scenarios. It should also function as a transparent and collaborative educational tool that allows the public to submit scenarios for ONC review and that shares with the public ONC’s interpretation of such scenarios.

In this section of the rule, ONC notes that any analysis of information blocking necessarily requires a careful consideration of the individual facts and circumstances, including whether the practice was required by law, whether the actor had the requisite statutory knowledge, and whether an exception applies. We support ONC’s careful and methodical approach to enforcement. We urge ONC, along with the Office of the Inspector General (OIG), to provide additional assurances to physicians that if they try, in good faith, to comply with an exception or otherwise not engage in information blocking and do their due diligence (e.g. document relevant decision-making and steps taken along the way), that such evidence would be strongly considered when making a determination about information blocking. Further, we ask for clarification on the guardrails of data blocking if health systems and providers decided to not work with a specific application, for a variety of reasons, including questionable clinical content or unknown algorithms or methodology. This
decision, when documented clearly, should not constitute data blocking. We also remind ONC that it should only hold accountable stakeholders who actually have direct control to enable information blocking.

The ACS also strongly urges ONC to help ensure that physicians are well-educated on the best approaches to securing and exchanging patient health information and to ensuring that access is only granted to those who should have access. The regulations proposed in this rule are not only complex and confusing, but they represent a major paradigm shift for data sharing. Currently under HIPAA, the presumption is that a physician cannot share patient health information unless he/she has a permissible purpose for sharing such data, and can only do so with a limited set of individuals and organization types. However, the provisions in this rule take the opposite approach by creating the presumption that patient health information must be shared with a variety of entities for a variety of purposes unless one of the information blocking exceptions is met. Going forward, ONC must clearly and comprehensively educate physicians so that they can better navigate the divergence and conflict between HIPAA and the updated Information Blocking regulations to know when and with whom it is appropriate to share data and when it is inappropriate. Special attention must be paid to smaller practices which may be at increased risk for violations simply because they do not have the resources to manage compliance. We strongly recommend that ONC focus its initial efforts on educating physicians about their responsibilities under these new regulations rather than fines or other disincentives related to information blocking. Given this need, ACS recommends delaying the timeline for this proposal. Currently, ONC plans to implement the information blocking regulations on the effective date of the final rule. We suggest delaying the implementation to be 18 months from the effective date of the rule to allow for adequate time to train providers on these updated regulations.

Additionally, we think it is critical for ONC and CMS to work with Office for Civil Rights (OCR), the Office of Human Research Protections (OHRP), and the Federal Trade Commission (FTC) to carefully re-assess regulations which were not created within the scope of the current digital landscape. While we recognize that a complete overhaul of these long-standing regulations might be challenging, at the very least, HHS should aim to eliminate conflicts and duplication across federal and state privacy laws. Currently, HIPAA covered entities and their business associates
must comply with a complex framework of laws and regulations that include the HIPAA regulations, the Common Rule, the FTC Act, state regulations, and now, if finalized, these new information blocking regulations. While we appreciate ONC’s efforts to consult with OCR to develop the information blocking provisions consistent with HIPAA Privacy and Security Rules, the lack of harmonization within this vast framework of laws will create uncertainty and confusion for HIPAA covered entities and their business associates that want to exchange health information. The ACS also wants to ensure that registries, as organizations and tools used for quality improvement purposes, remain covered entities under all updated privacy regulations.

Finally, the ACS is concerned about the commitment of resources to ONC and OCR given the heavy lift of implementing and enforcing these proposed rules. Proposed budget cuts to ONC and the Office for Civil Rights (OCR), as currently proposed in the 2020 budget plan, could hinder the agencies’ efforts to implement and enforce this proposed rule. The proposed federal budget includes a 17% cut to ONC, from $60 million to $43 million, and a similar cut to OCR’s budget. Given the critical need for testing and validating the framework described in this rule, we question whether the proposed budget will cover the resources and capacity needed for a complete and thorough implementation.

**Relevant Statutory Terms and Provisions**

**Electronic Health Information (EHI)**

Since “EHI” is not specifically defined in statute, ONC proposes to define it as:

- ePHI; and
- Any other information that is:
  - Transmitted by or maintained in electronic media, as defined in 45 CFR § 160.103;
  - Identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
  - Relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
The ACS is concerned that this proposed definition of EHI is too vague, subjective, and potentially expansive for purposes of information blocking enforcement. As currently defined, EHI could include information on an individual’s health insurance eligibility and benefits, billings for health care services, and payment information for services to be provided or already provided, which may include price information. To limit confusion and regulatory burden, we recommend that the information blocking restrictions in this rule only apply to the data classes in the USCDI. HHS notes throughout the ONC and CMS rules that the USCDI is well-positioned to facilitate care coordination and to promote interoperability. This would help to ensure that physicians are only held accountable for data over which they have more direct control and would better align with the certified capabilities of health IT vendors as proposed elsewhere in this rule regarding APIs.

Health Care Providers, Health IT Developers, Exchanges, and Networks

ONC proposes to adopt a definition of “actors” that is consistent with the four classes of individuals and entities mentioned in the Cures Act: 1) health care providers; 2) developers of certified health IT; 3) health information networks (HINs); and 4) health information exchanges (HIEs). According to ONC, the defining attribute of a “HIN” is that it enables, facilitates, or controls the movement of information between or among different individuals or entities that are unaffiliated. “HIE” is more narrowly defined as an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes. ONC cites a clinical data registry as an example of an HIE, since it might facilitate or enable the access, exchange, or use of EHI for a limited scope of participants and purposes.

The ACS has serious concerns that the broad definitions of both “HIE” and “HIN” have the potential to inappropriately hold clinical data registries responsible for complying with the data blocking restrictions in this rule. Clinical data registries are typically repositories of data gathered from other primary sources. Their primary goal is not patient-level data-sharing to facilitate direct patient care. Rather, registries are meant to capture broader trends and facilitate improved quality of care for populations of patients. In fact, for many ACS clinical data registries, it is not a requirement to enter PHI, and it is often not entered as part of quality improvement practices. In this section of the rule, ONC clarifies that EHI would not include health information that is de-identified in accordance
with HIPAA. Given the role and function of registries and ONC’s definition of EHI, the ACS believes it is unreasonable to hold registries accountable for complying with the information blocking provisions in this rule and for ensuring that patient-specific data is easily and regularly accessible to the patient or a third-party requestor.

We also request clarification from ONC on whether its definition of HIEs or HINs would cover payers and thus, include them on the list of “actors” subject to the information blocking provisions. Our interpretation of the rule is that the information blocking provisions do not apply to payers. Since health plans originate and manage large amounts of patient data and many of the proposals in both the ONC and CMS rule would require plans to share such data, it is critical to hold payers accountable for complying with the information blocking provisions.

Finally, the Cures Act specifically defines actors that may engage in information blocking and that would be subject to the information blocking restrictions set forth in the rule. However, neither the statute nor the proposed rule clearly defines to whom these actors are obligated to make data accessible. For example, is a physician obligated to make data available to a third-party app developer if authorized by a patient? In its discussion regarding authentication, ONC discusses how an app has to request that the FHIR server provide information about the patient record. Could a physician who has adopted and deployed CEHRT with FHIR-based API technology reject such a request from an app developer without being accused of information blocking? Would the physician have to claim an exception (e.g. that the request is infeasible) in order to reject the request? And, we seek clarification from ONC on whether it is the actual data that the physician is obligated to make available to the third-party app developer or simply the data integration capabilities already embedded in the API? Similarly, is a physician obligated to make a patient’s identifiable health information available to payers? The proposals in the ONC and CMS rule will likely empower payers to demand more information than is needed, which has the potential to lead to inappropriate use of data in determining coverage and/or physician reimbursement. Could the physician be accused of information blocking if he/she denied a payer access to a patient’s data? Must the physician claim one of the information blocking exceptions (e.g., protecting patient privacy) in order to deny a payer’s request for EHI and avoid being accused of information blocking? Generally, ACS is concerned that the current language does not allow a provider to use clinical judgment to deny access to patient-level
health data to a third-party app or payer, even if their use of the data is unknown or inappropriate.

Price Information

ONC seeks comment, for future rulemaking, on the parameters and implications of including price information within the scope of EHI for the purposes of information blocking. The ONC acknowledges that the fragmented and complex nature of pricing within the health care system creates challenges for patients and health plan sponsors in anticipating, lowering, comparing and planning for costs. The ONC indicates that an important goal of transparency in the price and cost of health care is to empower patients to make informed health care decisions. The ONC also states that the availability of price information could help increase competition that is based on the quality and value of the services that patients receive.

We support the concept of increased price transparency, but we urge the ONC to consider the context in which such data are shared and the minimization of burden on providers as they seek to comply with any new requirements. We provide some overarching comments on price transparency:

- **Quality data are also needed to understand cost.** To truly understand value, accurate and reliable information on both quality and cost are required, and ideally quality and cost should be measured over the same period of time for the same episode of care. Unfortunately, many data gaps exist regarding the quality of individual physicians, and data that are in fact available are often unreliable or limited in scope. Also important is the timeframe for assessing quality. As an example, a prominent cancer hospital was examined for the annual cost of care provided for breast cancer treatment and was found to be one of the most expensive centers nationally. But when the cost was examined over 10 years, as opposed to 1 year, the center was found to have much lower costs than other centers during this longer time period due to the high quality of care provided and low cancer recurrence rates. Although in the first instance the value appeared to be low, when taking a longer view of the time period, the center was found to provide extremely high value care. Therefore, one aspect of assessing quality includes considering the appropriate time window for a true picture of value. The ONC states that a goal of price transparency is to empower patients to make health care decisions; as such, the
ONC should give careful consideration to sharing of price data that cannot be reliably paired with accurate and relevant quality data.

- **Start small.** Much of the provision of health care involves tests and quick services such as lab tests, CT scans, or other diagnostic tests. Sharing the prices for this information could be relatively straightforward and useful to patients, despite lack of corresponding quality data. Similarly, cost information on annual exams or other commoditized care, such as colonoscopies, could be helpful and easier to share with patients, unlike the costs of complex care such as cancer treatment, which warrant information on quality as well to make assessments of the value of the care.

- **Clinicians should not be held responsible for sharing price information.** The responsibility of sharing cost information should rest on payers, not providers. Requiring providers to seek out cost information from payers will slow down patient care and represent an increased burden for providers. Providers should also not bear the burden of explaining health care pricing to their patients. Providers might not even have up-to-date knowledge of a patient’s costs; rather, the payer is in the best position to share the most definitive information on the patient’s coverage, services that have received prior authorization, co-payments and deductibles, and out-of-pocket costs. However, health plans are not listed as “actors” under the information blocking proposals. As we mentioned earlier, ONC should consider adding these organizations to the list of actors in order to enable patients to obtain accurate and up-to-date cost information.

The proposed rule sets forth a number of questions on the technical, operational, legal, cultural, environmental, and other challenges to creating price transparency within health care, many of which we address below:

1. **Should prices that are included in EHI:**

   - **Reflect the amount to be charged to and paid for by the patient’s health plan (if the patient is insured) and the amount to be charged to and collected from the patient (as permitted by the provider’s agreement with the patient’s health plan), including for drugs or medical devices?**

Health plans would be in the best position to provide accurate and up-to-date information on the amount to be charged to and paid for by the patient’s health plan. In both instances, we urge the ONC to require that health plans, not providers, communicate this information to patients.
• Include various pricing information such as charge master price, negotiated prices, pricing based on CPT codes or DRGs, bundled prices, and price to payer?

The charge master price, negotiated prices, and bundled prices without context are less useful for patients, or worse, could be misunderstood. Providing pricing information based on CPT or DRGs could be more helpful in some circumstances (i.e. comparing the cost of a colonoscopy across payers), but in cases of complex care, a single CPT or DRG is just one part of a larger picture. Alternatively, the cost of an entire episode of care could prove to be the most informative and actionable price information for patients. Our research shows that when patients undergo an episode of care over 90 days, they receive a large number of services spanning tests (lab, CT, MRI, etc.), consults, drugs, anesthesia, skilled nursing facility care, home health care, long term acute care, etc. It would be overwhelming for a patient to receive and understand the cost information for each service.

The best approach is to create patient awareness of what the entire cost of care is likely to be, based upon their prognosis, risk factors, and other characteristics. Figure 2 below shows cost expressed in terms of the continuum of time and services provided within an episode of care. This example shows the total cost for all services within an episode, with care provided by multiple TINs. The figure also shows the patient’s portion of costs according to their benefit plan, i.e. their out-of-pocket costs. ACS is working with the CMS Episode Grouper Methodology (EGM) to create a public utility for all patients to have available episode-based reference pricing. We are seeking government involvement to make this information available to all patients. If HHS is contemplating moving beyond fee-for-service, then providing bundled prices, rather than vast amounts of information on prices on individual services, is needed to truly inform patients of the cost of their care.
• Reflect all out-of-pocket costs such as deductibles, copayments and coinsurance (for insured patients) and/or include a reference price as a comparison tool such as the Medicare rate and, if so, what is the most meaningful reference?

Out-of-pocket cost information is one of the most useful types of price information for patients as they make health care decisions. A benchmark price is required to provide context when making cost (beyond out-of-pocket costs) available for a service or an episode, or anything in between. The Medicare rate is a reasonable benchmark price. It is also possible to more accurately estimate patient total cost of care for an episode by incorporating patient’s risks and comorbidities into the price reports.

2. For the purpose of informing referrals for additional care and prescriptions, should future rulemaking by the Department require health IT developers to include in their platforms a mechanism for patients to see price information, and for health care providers to have access to price information, tailored to an individual patient, integrated into the practice or clinical workflow through APIs?

Price information for an individual patient that is integrated into providers’ clinical workflow through APIs would be useful information for referrals for additional care and prescriptions. We urge ONC to support the development and use of platforms such as the product created by Gemini Health, which aims to reduce health care costs through drug cost transparency at the point of care in a clinical workflow integrated within
EHRs. The ability to access patient-specific drug and alternative cost and coverage information at the point of care reduces pharmacy call backs, prior authorizations, and patient frustration. If patients have increased information about comparative treatment options and medications, protections should be put in place to ensure that clinicians are not required to provide alternatives that the clinician does not deem appropriate, nor should clinicians be held liable for refusing to offer such alternatives.

3. To the extent that patients have a right to price information within a reasonable time in advance of care, how would such reasonableness be defined for:

- Emergency care, including how and when transparent prices should be disclosed to patients and what sort of exceptions might be appropriate, such as for patients in need of immediate stabilization;
- Ambulance services, including air ambulance services; and
- Unscheduled inpatient care, such as admissions subsequent to an emergency visit?

We are concerned about trends in payment for emergency care, specifically the refusal of some commercial payers to pay for emergency care when it was later discovered that the patient did not in fact have an emergency medical condition. For example, if a patient thought she was having a heart attack, but the patient was in reality experiencing indigestion, we do not believe that the patient should bear the cost of the emergency care and ambulance services because this could discourage patients who are truly having an emergency from seeking emergency care. Given these concerns, we believe emergency, ambulance, and air ambulance price information should be excluded from the information blocking prohibition.

4. How would price information vary based on the type of health insurance and/or payment structure being utilized, and what, if any, challenges would such variation create to identifying the price information that should be made available for access, exchange, or use?

ACS has used the EGM and analyzed patients engaged in episodes of care. The number of Tax Identification Numbers (TINs) which touch a patient within an episode of surgical care may vary from as few as a couple to as

---

many as 50 or more. For a patient to have a reasonable sense of price in fee-for-service models for all the services used in an episode would overwhelm the patient with information. ACS prefers for CMS to represent price to patients using condition episodes or procedure episodes which represent an average price for the sum of all services typically provided for patients with their condition or procedure. For example, a breast cancer patient or colon cancer patient will have multiple services to establish a diagnosis, stage their disease and prepare the patient for chemotherapy, radiation therapy and/or a surgical procedure. In addition, the patient’s co-morbidities will also influence the overall price. The ACS is working to bring the CMS EGM into public use for such patients to establish their condition or procedure price average for Medicare as a benchmark. These average prices can be further modified as a percentage of Medicare for those commercial rates which are based off Medicare rates.

The CMS EGM is the most informed and comprehensive approach to providing patients with average price information. It can be further advanced by deploying the algorithms inside Accountable Care Organization (ACO) data or larger claims databases such as in Fair Health or in Cerner’s HealthIntent. ACS encourages ONC and CMS to work to further this utility as a public service for all patients.

Such a standard in the industry would allow plans to provide patients with a patient-specific price estimate for the services on which they are seeking price information. We stress that insurers and not providers should be responsible for accessing and sharing price information with their patients. At the most, providers should share a benchmark price, based on a Medicare benchmark, so that patients have a way to compare the price information from the health plan.

5. **Should price information be made available on public web sites so that patients can shop for care without having to contact individual providers, and if so, who should be responsible for posting such information? Additionally, how would the public posting of pricing information through API technology help advance market competition and the ability of patients to shop for care?**

Yes, we strongly support the availability of price information on public websites. However, doing so for singular events of care such as in fee-for-service is only valuable to patients when the services provided are typically stand-alone. Much of care is not suited for fee-for-service stand-
alone events and would be more informative to patients to aggregate their total cost of care using the EGM. The ACS is engaging in efforts with multiple partners to create a public utility for EGM-based benchmark pricing leveraging the Medicare dataset. Until such public utility is developed, we stress that the responsibility of sharing cost information should rest on payers; patients should not be required to contact individual providers for their cost information. Payers should be responsible for posting such information based on a standard grouper methodology such as EGM because they will have the most accurate and up-to-date knowledge of the costs of a given episode of care and other patient costs. Again, we note that health plans are not listed as “actors” under the information blocking proposals, so ONC should consider adding these organizations to the list of actors in order to enable patients to obtain cost information. The public posting of pricing information through API technology can help advance market competition and the ability of patients to shop for care if the data that are presented include the appropriate contextual information (quality data, benchmarks, etc.) so that the pricing information can be interpreted correctly and is not misleading.

6. How can price transparency be achieved for care delivered through value-based arrangements, including at ACOs, demonstrations, and other risk-based sharing arrangements?

As we stated above, to truly understand value, accurate and reliable information on both quality and cost are required. The ONC states that a goal of price transparency is to empower patients to make health care decisions; however, providing certain types of cost information without additional context could result in patients misinterpreting the information. In the case of value-based arrangements such as ACOs, demonstrations, and other risk-bearing arrangements, patients should receive some background information as to the goals and structure of the arrangements. Patients should also receive information on the included quality measures and other safeguards against stinting as a way for providers to reduce cost.

The work mentioned previously to leverage the clinical information and grouping logic in the EGM also applies to ACOs and other value-based payment arrangements. This ongoing work is intended to be broadly applicable across payers and regardless of payment arrangement. Today, ACOs frequently lack the expertise to analyze the cost of specialty care and therefore frequently fail to identify and target cost drivers such as unwarranted variation. Grouping of services into logical episodes of care in a manner that avoids double counting of costs will provide valuable information to providers participating in value-based payment
arrangements. These insights could be passed along to the patient as well. For example, the information generated could be used by the ACO or other payment arrangement to provide a patient-specific estimate of out-of-pocket costs for their entire care journey for a condition or procedure.

7. If the price information is included in EHI, could that information be useful in subsequent rulemaking that the Department may consider in order to reduce or prevent surprise medical billing?

Surprise medical billing is a consequence of current insurance plans offering overly narrowed networks. Surprise billing is the mischaracterization of surprise benefits in which insurance companies have faultily narrowed provider networks in order to reduce premium costs and to create high deductible plans. This failure of insurance companies has created the surprise medical billing crisis. The solution is not to increase the availability of price information, but to create better benefit design and improved insurance coverage.

Observational Health Information

ONC highlights that blocking observational health information which is collected or maintained during the practice of medicine or delivery of care is of special concern because it has the potential to interfere with the access, exchange, or use of EHI. ONC also explains that practices related to electronic non-observational health information typically would not implicate the information blocking provision—such as population-level trends, EHI used for comparisons and benchmarking activities, quality measures and other care protocols. As discussed in section VIII.C.5.c in this rule, while we agree that the non-observational data examples provided by ONC should not be subject to the data blocking provision, ACS wants to ensure that ONC has a clear understanding of the type of data that are collected by clinical data registries, especially within the context of non-observational data. ACS clinical data registries and other similar registries should not be subject to information blocking provisions because it is not a requirement that registries enter or retain PHI, and most registry participants do not enter or retain PHI as part of their quality improvement practices. It should also not be expected that registries share data they have received from other sources, as that goes beyond their scope. We do not believe that it was the intent of Congress to have these type of QI initiatives subject to such regulations because the threat of data blocking provisions could hamper the trusted relationship the provider has with clinical data registries as an information source to drive
improvements in care. Therefore, we encourage further clarification and examples from ONC to help with public assurances that these data are not subject to data blocking provisions.

ONC also notes that practices related to electronic non-observational health information such as price information, could still be subject to the information blocking provision. **ACS strongly opposes that pricing information be subject to the information blocking provisions.** As discussed above in the Price Information section, pricing information should never be shared in isolation without reliable and valid information on the quality of care.

**Proposed Exceptions to Information Blocking**

In this rule, ONC proposes seven exceptions to the general prohibition on information blocking, which are discussed below. Although ONC provides some examples of what would constitute information blocking, it relies more heavily on describing reasonable and necessary activities that would not count as information blocking. ACS believes this strategy is confusing and that it leaves a considerable amount of grey area in terms of what would qualify as an “exception” and what would not. If ONC finalizes these exceptions, we recommend that it provide additional guidance with more specific examples of activities that would qualify for each exception and more specific instructions on the steps physicians and other stakeholders would need to take to demonstrate compliance with each exception. It is critical that ONC adopt a transparent process that requires actors to clearly document their rationale for claiming an exception to ensure the legitimacy of such claims. As discussed in an earlier section, the ONC publishing specific examples of what constitutes data blocking and what constitutes exceptions will facilitate a better understanding of how to operate and practice within these updated regulations, and to ensure claims of both data blocking and its exceptions are legitimate and appropriate.

ONC also proposes that in order to qualify for any of these exceptions and to avoid potential civil penalties and other disincentives under the law associated with information blocking, a regulated actor would, for each relevant practice and at all relevant times, have to satisfy all of the applicable conditions of the exception. The ACS is concerned that this requirement sets an unrealistically high bar for individual physicians, who may not have the same level or access to resources as hospitals or health IT vendors. As mentioned earlier, the information blocking restrictions proposed in this rule are vague and confusing, which could result in well-
intentioned physicians being inappropriately implicated simply due to a lack of clarity regarding their role and responsibilities. Steps should be taken by ONC to ensure that physicians are not unduly burdened by compliance.

Also, as noted earlier, the proposed information blocking requirements create tension with existing HIPAA requirements, which will be challenging for physicians to navigate. To ensure that physicians adhere to these requirements, but are not consumed by compliance, ONC should clarify that physicians providing the minimum necessary information to an actor (even a covered entity) will not be considered an information blocker without having to go through the exercise of meeting the requirements of the sub-exception. Payers, in particular, may feel empowered by these rules to demand more information from a physician than is needed. ONC should clarify that a physician’s professional judgment to protect their patients’ rights or privacy will never be considered information blocking, and not require a physician to walk through the steps of the sub-exception.

ONC’s proposed exceptions to the general prohibition on information blocking are discussed below:

1. **Preventing Harm.** This proposed exception acknowledges that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of EHI. For example, this exception may be relevant if certified health IT were to incorrectly present an old and superseded version of a medication list, or when only partial copies of laboratory tests are being linked to a patient when the patient’s record is exchanged. In general, the ACS supports making an exception for practices necessary to prevent harm to patients. However, we do want to ensure that there is a clear difference between historical data and inaccurate data, and ask that this definition be further clarified. Otherwise, historical data could be withheld and claimed it fell under this exemption. We also support ONC’s definition of “harm” to include corrupt or inaccurate data being recorded or incorporated into a patient’s EHR, as well as the misidentification of a patient’s EHI. The accuracy of EHR data is critical not only for patient safety, but to ensure that analyses and other healthcare quality and safety interventions based off these data are accurate and effective.

2. **Promoting the Privacy of EHI.** According to ONC, this proposed exception would advance the goal of preventing information
blocking for improper or self-interested purposes while maintaining and upholding the privacy rights that patients now have. The ACS supports efforts to promote the privacy of EHI, but we are concerned that health IT vendors may inappropriately refuse to share PHI based on the false premise that such transfer of data somehow violates HIPAA. We urge ONC to advise health IT vendors that HIPAA compliance is not a justification for withholding data from entities, including clinical data registries, if such entities are in compliance with all applicable HIPAA Rules.

**ONC also should clarify that a physician’s professional judgment to protect their patients’ rights or privacy will never be considered information blocking, and not require a physician to walk through the steps of the sub-exception, which specifically requires an individual to ask that the information not be accessed, exchanged, or used.**

As discussed as a general concern throughout this letter, ACS recommends reviewing and updating all existing privacy regulations to ensure all are consistent, and that there are no discrepancies in expectations between them. This includes HIPAA, 42 CFR Part II, the Common Rule, and IRB regulations; all should be updated and adjusted in order to accommodate the more expansive capabilities of electronic data exchange. We also believe that this exception indicates a clear need to certify that apps meet privacy standards, in addition to the certification that applications meet technology and clinical logic standards, discussed above.

3. **Promoting Security of EHI.** This proposed exception is intended to protect actors who mitigate security risks and implement appropriate safeguards to secure the EHI they control. Similar to our comments above, the ACS supports ONC’s efforts to promote the security of EHI, but we are concerned that HIT vendors may inappropriately deny access to data based on the false premise that such transfer of data somehow violates HIPAA. Again, the ACS urges ONC to advise HIT vendors that HIPAA compliance is not a justification for withholding data from entities, including clinical data registries, if such entities are in compliance with all applicable HIPAA Rules.

However, ACS is also concerned about the security of EHI once it moves beyond what is covered under HIPAA, and is under control of vendors and products in the health IT space, including mobile applications. While we understand that this is outside of the ONC’s purview, it is critically
necessary for the government to facilitate the development of privacy certification for mobile apps to include clear requirements on how they communicate data use and privacy to users. We encourage ONC to look to the existing FDA process as a model for the certification of mobile health apps for the provisions in this rule. For mobile apps that do not sufficiently meet these suggested standards, providers and organizations should be able to utilize this exception to not share health data with these products.

4. **Recovering Costs Reasonably Incurred.** According to ONC, this proposed exception acknowledges that actors should be able to recover costs that they reasonably incur to develop technologies and provide services that enhance interoperability and promote innovation, competition, and consumer welfare. ACS appreciates the intent of this exception, but we do not believe that the language is prescriptive enough. Although the new certification criteria proposed in the ONC rule are intended to support greater interoperability and protect against inappropriate data blocking, they will require a significant investment of resources on the part of health IT vendors. These costs will almost certainly be passed on to the health IT user and this exception gives vendors a pass to do that. As discussed elsewhere in this comment letter, API Data Providers (i.e., “physicians”) will be responsible for covering the bulk of these costs since they are mandated to use CEHRT, required to make data accessible via APIs, and are limited in their ability to recoup the costs of complying with these requirements from patients and potentially from API Users (i.e. third-party app developers). To minimize unreasonable charges and the impact this could have on HIT users, such as physicians, it is critical that ONC adopt transparency requirements for vendors to clearly disclose the methodology of their fees. ONC also should adopt an objective and verifiable process to specifically evaluate whether the fees that vendors are charging are truly reasonable and are being applied fairly and uniformly across similar stakeholders.

At the same time, we believe that ONC is overlooking a larger, more fundamental problem, which is the ongoing lack of industry standards for data exchange and interoperability. In this rule, ONC proposes to require the adoption of FHIR-based APIs. However, not all FHIR servers are created equally. Additionally, FHIR has multiple versions, and will continue to grow and adjust to needs over time, creating challenges with semantic versioning. **Until the government sets more formal standards around interoperability and data exchange, including standards for APIs, we will continue to see a proliferation of costly, non-**
standardized, proprietary systems, just as we saw a proliferation of proprietary EHR technology following the passage of the HITECH Act, and physicians will continue to bear the burden of covering these costs. If the federal government were to adopt a more uniform set of standards that certified EHR technology was required to adhere to, costs would be more predictable and it would be more difficult for health IT vendors to block data exchange through the imposition of unreasonable charges.

5. **Responding to Requests that are Infeasible.** This proposed exception acknowledges that there may be legitimate practical challenges beyond an actor’s control that may limit its ability to comply with requests for access, exchange, or use of EHI. The ACS is concerned that health IT vendors may attempt to use this proposed exception to inappropriately deny clinical registries access to data. It is important that ONC enforce its policy that in the event that an actor determines that providing data in a particular manner is not feasible, it must provide the requestor with an explanation of the reasons why the actor cannot accommodate the request and it must work with the requestor in a timely manner to provide a reasonable alternative means of accessing, exchanging, or using the EHI.

6. **Licensing of Interoperability on Reasonable and Non-Discriminatory Terms.** This is another fee-based exception that would protect “reasonable” royalty fees associated with licensing and use of interoperability elements. ONC defines “interoperability elements” to include any means by which EHI can be accessed, exchanged or used, and ONC clarifies that the definition is not limited to functional elements and technical information, but also includes technologies, services, policies, and other conditions necessary to support the access, exchange or use of EHI. To receive protection under this exception, the actor would have to respond to requests within 10 business days by negotiating in a reasonable and non-discriminatory fashion to identify the elements needed and to offer a license with reasonable and non-discriminatory terms. ONC sets out parameters concerning such terms that relate to, among other things, the scope of rights to be licensed, the royalty that would be permitted, collateral terms, and non-disclosure agreements that only narrowly protect unauthorized disclosure of the actor’s trade secrets. ACS supports the intent of this proposal, however we have concerns that the term “reasonable” is not defined and therefore these cases could lead to
countless court cases. This is particularly concerning because the clients of EHR vendors and registries cannot easily move from one vendor to another since the client’s data are held within the EHR or registry and in most cases the cost and resources needed to move and translate these data are massive. Therefore, in order to resolve this issue, we ask ONC to explore a policy that would require vendors and registries to accept a binding arbitration with a national arbiter which would then lead to legal precedence. It is important that these cases are not endlessly held up in court, while also not stifling innovations that are the product of a free market.

7. Maintaining and Improving HIT Performance. This exception would permit making health IT temporarily unavailable for maintenance or improvement purposes, subject to certain limitations. To qualify for this exception, the unavailability of health IT for maintenance or improvements must be:

- For no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable
- Implemented in a consistent and non-discriminatory manner
- Agreed to by the individual or entity to whom the health IT is supplied (this condition does not apply when health IT is made unavailable for maintenance or improvements at the initiative of a recipient (e.g., customer) of health IT)

ACS supports an actor’s ability to make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the practice is for a period of time no longer than necessary and implemented in a consistent and non-discriminatory manner. We urge ONC to require that actors provide advance notice that health IT will be temporarily unavailable in order to perform maintenance or improvements when feasible.

Information Blocking Enforcement Mechanisms

The OIG has both investigatory and enforcement authority over information blocking and may issue civil money penalties ($1,000,000 per incident) for information blocking conducted by health IT developers of certified health IT, health information networks, and health information exchanges. The OIG may also investigate health care providers for
information blocking for which health care providers could be subject to disincentives. ONC clarifies that health care provider penalties will be established in future rulemaking.

ACS requests that ONC provide more explicit details about how it plans to work with OIG to police these provisions since the rule provides little details. ACS recommends creating a panel or advisory board with both physicians and vendors to determine and set reasonable penalties and other disincentives, as well as delaying penalties to begin 6 months after the implementation of the updated data blocking provisions to better understand the challenges and the practical implications. ONC also seeks comment on potential disincentives for providers. From the physician perspective, providers will take steps to limit their vulnerability to being subject to civil money payments, including smaller physician groups going back to paper and leaving EHRs.

The information blocking proposals also provide for a complaint process and corresponding confidentiality protections to encourage and facilitate the reporting of information blocking. ONC proposes to build on existing mechanisms, including the complaint process currently available via the ONC Health IT Feedback Form. As we noted earlier, it would be extremely helpful if ONC could incorporate into this process a publicly-accessible, searchable, and living repository of examples of activities that do (and do not) constitute information blocking. In addition to allowing for the submission of formal complaints, including the status of those complaints, this tool also should provide the public with an opportunity to share with ONC for review specific actions that a stakeholder may be considering.

Registries Request For Information

The Cures Act focuses on interoperability and bidirectional exchange between EHRs and registries, including clinician-led clinical data registries. ONC seeks information on how health IT solutions and the proposals throughout its proposed rule can aid bidirectional exchange with registries for a wide range of public health, quality reporting, and clinical quality improvement initiatives (e.g., do proposed standards for certified APIs have the potential to change how information is exchanged with registries?).

It is essential that ONC address both the ability of EHR vendors to exchange EHI, as well as the usability of the exchanged information. Lack of interoperability between EHRs and other health IT and registries
impedes the collection and analysis of data needed to accurately assess and appropriately improve quality of care. While many registries have found methods to work around this lack of interoperability, such efforts have required significant investments of time and resources. Improved interoperability would allow registries to conduct their work more efficiently and effectively, reduce administrative burden, and devote more time and resources to analyzing data to identify best practices and improve patient care, as well as ensure that the data are current, relevant, and complete. A regulatory framework that focuses on improving the exchange of EHI with registries and the usability of such data will assist efficient exchange of information and allow providers and clinicians to more effectively make use of registries for reporting under the MIPS Program, as well as the promotion of research, public health, and quality improvement activities by registries.

In this rule, ONC specifically seeks information about how ONC’s proposed new standards and capabilities for certified APIs to aid bidirectional exchange of data with registries, as well as use cases where an API using FHIR Release 4 might support improved exchange between a provider and a registry. The ACS supports moving to this standard, though wants to ensure that appropriate time is given to test updated standards and ensure that FHIR allows for the exchange of bulk data for registries. Additionally, the goal of semantic interoperability through APIs, however, will only go so far without natural language processing or human curation of clinical notes, both of which are resource intensive and often unsuccessful. ONC has skipped straight to APIs and FHIR as the solution to interoperability challenges, but many entities lack standardized and codified data elements. Development of these resources is often very costly and requires technical support. As a result, ACS urges ONC to provide technical assistance for organizations looking to develop HL7 standards, and provide enough time for vendors and registries to thoroughly test new standards to ensure registries are receiving all of the required data with a lower administrative burden.

Overall, ACS recommends developing and enforcing standards for APIs to FHIR and limiting EHI to USCDI data elements. By enforcing standards for data exchange and requiring EHRs to include the ability to incorporate external data into their systems after a clinical review process and facilitated by a standard cloud platform, interoperability will be achievable and scalable.
Patient Matching Request For Information

In coordination with CMS rule, ONC seeks to better understand the patient matching landscape and to identify areas where ONC can assist in standards and technical development, coordination, and innovation. We agree that patient matching is a critical issue, and are concerned with patient safety issues that could occur as a result of inaccurate matching, including but not limited to inappropriate or duplicative care leading to increased costs, increased burden on patient and provider to ensure accurate data in shared records, and incomplete information. In the absence of a legislative fix such as a UPI for this issue, the ACS recommends that CMS and ONC continue to explore alternative solutions for this problem. A standard algorithm hosted in a cloud platform that assesses and determines patient matches based on identifying information, such as name, date of birth, Payer ID, or other unique identifiers could be a stop-gap solution. Further, standard requirements for patient identifiers as part of the USCDI, such as number of digits and inclusion of hyphens, dashes, and apostrophes, could aid in this issue by standardizing the name field in EHRs and apps. However, these options will not solve this problem completely, and ACS encourages a larger legislative fix for this issue, as it will only grow in size as digital technology continues to increase in scope and practice.

The ACS appreciates the opportunity to provide feedback on this proposed rule and looks forward to continuing dialogue with ONC on these important issues. If you have any questions about our comments, please contact Jill Sage, Quality Affairs Manager, at jsage@facs.org.

Sincerely,

David B. Hoyt, MD, FACS
Executive Director